NASA Procedural Requirements

NPR 8000.4
Effective Date: April 25, 2002
Expiration Date: April 25, 2007

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Subject: Risk Management Procedural Requirements w/Change 1 (4/13/04)

Responsible Office: Office of Safety and Mission Assurance

CHAPTER 2. Implementing the Risk Management Process

2.1 Overview of the Risk Management Process

2.1.1 RM begins early in program/project formulation and must continue in a disciplined manner throughout all program/project life cycle phases. A long-range view of the program/project and its mission success criteria, and open communication among all members of the program/project team (including stakeholders), are essential elements for successful RM.

2.1.2 Although different organizations refer to RM elements by different names, RM processes used for years by various organizations contain virtually the same essential core ingredients. For example, the IT security process as described in NPR 2810.1 considers threats (equivalent to undesirable events as used in the definition of risk in this NPR and NPR 7120.5), vulnerability (equivalent to likelihood (see Appendix A, Glossary) of occurrence as defined in this NPR) and impact (equivalent to consequences as defined in this NPR) as the key elements in identifying risk. The RM process identified in Figure 1 contains the basic elements of the process. Users may substitute other nomenclature as long as the requirements of all elements are satisfied. Details on each step of the process are provided in the following paragraphs.

2.2 Risk Identification

2.2.1 Risk Identification Concept.

The first step in the RM process is to identify the risks (technical and programmatic) specific to a program/project. As identified in NPR 7120.5, this entails identifying individual risks and clearly describing those risks in terms of both the undesirable event the risk presents as well as the consequences of that event to the program/project. In addition, risk identification includes identification of all the necessary information to place the risk in the context of the program/project. This is necessary to ensure that the original characterization of the risk can be understood by other personnel, particularly after time has passed. Risk identification shall be continued throughout the life cycle of the program/project. (Requirement 26015). In identifying risks, PM's should challenge even those things that have long worked successfully, and ask at least the following questions:

- "What can go wrong?"

- "What would be the consequences (to safety, mission objectives, schedule, cost) if it does go wrong?"

2.2.2 Risk Identification Inputs.

There are many useful sources of information that provide the input for risk identification, including the following:

a. Team members.

b. Previous analyses, lessons learned, and historical data. NOTE: Lessons learned from past projects are available from the NASA Lessons Learned Information System (LLIS) at: http://llis.nasa.gov/.

c. System safety and reliability analyses; e.g., hazard analysis, fault tree analysis, failure modes and effects analysis.

d. Expert interviews and external review boards (the NASA LLIS also provides access to selected Mishap Investigation Board Reports).

e. Data extrapolation based on review and analysis of compiled risk data.

f. Simulations, test data, and models.

g. Analysis of the work breakdown structure.

h. Comparison of mission objectives/success criteria, goals, assumptions, plans, and margins (maintained to address the "unknown unknowns").

i. Analysis of resources/schedule-review and analysis of required or available resources; continued monitoring of schedule milestones, and risk mitigation/planned action milestones.

j. Analysis of suppliers-review and analysis of the procedures and customer requirements of suppliers.

k. Analysis of proposed changes.

l. Test results.

m. Nonconformance reports.

n. Analysis of external factors that affect program/project risk; e.g., computer security assessments, physical security assessments, human factors performance assessments, environmental assessments.

o. Results of risk analyses from other programs, projects, and institutional areas that support or are critical to this program/project's success (for example, if a project requires the use of a test stand to perform critical tests and the test stand is currently undergoing refurbishment, the risks of completion of that refurbishment by the time needed for this project should be considered).

p. Risk understanding resulting from previous program(s) (heritage).

q. Tools and references as identified in Appendix D.

2.2.3 Risk Identification Outputs.

The primary output of risk identification is a statement of risk for each individual risk (see paragraph 2.7.5). These statements of risk are summarized in a comprehensive listing of program/project risks, or Risk List (see paragraph 2.7.6), which shall be established and maintained to reflect the current understanding of risks within the program/project (Requirement 26017).

2.3 Risk Analysis (Evaluation, Assessment, or Estimation)

2.3.1 Risk Analysis Concept.

In analyzing risks, PM's should ask at least the following questions:

How likely is it for this risk to occur?

How soon do we need to act on this risk?

How does this risk compare with other risks?

As identified in NPR 7120.5, risk analysis consists of estimating the likelihood and the consequences of the risk and the timeframe in which action must be taken on an identified risk to avoid harm. Estimates may be quantitative or qualitative, but should be stated and combined in such a way that identified risks can be prioritized (compared to each other or to relevant criteria and ranked from highest to lowest) in terms of mission impact. Methods of analyzing risk include, but are not limited to, the following:

a. Individual or group expert judgment.

b. Statistical analysis of historical data.

c. Uncertainty analysis of cost, performance, and schedule projections (consists of building and running a probabilistic model of the system under investigation, including the chance variation inherent in real-life cost, performance, and schedule).

d. Probabilistic Risk Assessment (PRA) (see Appendix A, Glossary) (also known as Probabilistic Safety Assessment (PSA) and Quantitative Risk Assessment (QRA)).

e. Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA).

f. Ordinal risk scales.

g. Comparison to analogous systems.

Before prioritizing, the risks should be classified or grouped with similar risks. There are several purposes for classification. One purpose of classification of risks is to understand the nature of the risks and to group related risks so as to build more cost-effective mitigation plans. Another purpose is to identify risks that are equivalent or duplicate each other and combine them as appropriate. Additionally, risks are classified so that they can be tracked and monitored by various elements of the program. For example, a functional area such as financial or safety may want to concentrate on the subset of risks within their functional area to assure that all these risks are adequately resolved. Perhaps all the risks related to the acquisition process maybe classified together for purposes of performing acquisition planning or source selection. Once classified, the risks should be prioritized. The purpose of prioritization is to sort through a large number of risks and determine which are the most important and, therefore, should be dealt with first.

One widely used qualitative method of prioritizing risks is through the use of a Risk Assessment Code (RAC). Other methods of prioritization include multivoting (quantitative) and attribute assignment (qualitative). The RAC method combines qualitative and semi-quantitative measures of risk likelihood with similar measures of risk consequences to yield a RAC that can be the basis for initial prioritization of risks. For example, a risk having a consequence of "Class II - Critical" and a likelihood of "A - Likely to occur," would have a RAC of 1, and would be a top priority for mitigation. The following paragraphs provide guidance in using the RAC. In addition, the RAC methodology can be tailored to fit the needs, complexity, or experience base of a program/project.

2.3.1.1 Consequence.

Consequence is an assessment of the worst credible potential result(s) of a risk. The measurement units differ depending on the specific risk. For example, the consequence of a cost risk may correspond to specific dollar amounts or percentages of the program/project budget or the consequence of schedule risks may correspond to the length of time delays. Consequence classifications are defined generally as Catastrophic, Critical, Marginal, and Negligible. A sample classification approach might be as follows:

a. Class I - Catastrophic. A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission; schedule slippage causing launch window to be missed; cost overrun greater than 50 percent of planned cost.

b. Class II - Critical. A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware; schedule slippage causing launch date to be missed; cost overrun between 15 percent and not exceeding 50 percent of planned cost).

c. Class III - Moderate. A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware; internal schedule slip that does not impact launch date; cost overrun between 2 percent and not exceeding 15 percent of planned cost.

d. Class IV - Negligible. A condition that could cause the need for minor first aid treatment but would not adversely affect personal safety or health; damage to facilities, equipment, or flight hardware more than normal wear and tear level; internal schedule slip that does not impact internal development milestones; cost overrun less than 2 percent of planned cost.

Note: The portions of these classifications concerning safety are defined within NPR 8715.3, "NASA Safety Manual."

2.3.1.2 Likelihood.

Likelihood is the probability that an identified risk event will occur. The following is as example of likelihood categories:

a. Likelihood A. Likely to occur (e.g., probability > 0.1).

b. Likelihood B. Probably will occur (e.g., 0.1 ≥ probability > 0.01).

c. Likelihood C. May occur (e.g., 0.01 ≥ probability > 0.001).

d. Likelihood D. Unlikely to occur (e.g., 0.001 ≥ probability > 0.000001).

e. Likelihood E. Improbable (e.g., 0.000001 ≥ probability).

2.3.1.3 Risk Matrix.

The risk matrix in Figure 2 shows the application of consequence and likelihood in determining a RAC and a qualitative (high, medium, low) risk rating.

	LIKELIHOOD ESTIMATE				
CONSEQUENCE CLASS	A	B	C	D	E
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	6
IV	3	4	5	6	7

High Risk	
Medium Risk	
Low Risk	

Figure 2. Risk Matrix Showing Risk Assessment Codes (RAC)

2.3.1.4 Timeframe.

Timeframe is the time in which action must be taken to handle the analyzed risk or the time period in which the program/project will be impacted by it. Timeframe may be used to order RAC's. For example, a RAC 1 risk with a "near-term" timeframe should be worked before a RAC 1 risk with a midterm or far-term timeframe. The following is an example of timeframe categories for a three year long program:

a. Near-term. The project must take action on the identified risk or will be impacted by the risk in the next 90 days.

b. Midterm. The project must take action on the identified risk or will be impacted by the risk in the next 90-180 days.

c. Far-term. The project need not take action or will not be impacted by the risk in the next 180 days.

2.3.2 Risk Analysis Inputs.

There are many useful sources of information that provide the input for risk analysis including the following:

a. Risk data generated in other steps in the process.

b. Test data.

c. Expert opinions.

d. Hazard Analyses, Failure Modes and Effects Analyses.

e. Lessons learned data and historical information from other programs/projects.

f. Probabilistic Risk Assessments (PRA).

g. Technical analyses resulting from other activities, for example electromagnetic compatibility/interference analyses, software verification and validation activities.

2.3.3 Risk Analysis Outputs.

The primary outputs of risk analysis are clear estimations of the consequences of the risk, the likelihood of the risk's occurrence, and the timeframe in which an action must be taken on an identified risk. This information is included and documented in the Risk List (see paragraph 2.7.6). Information obtained within the classification portion of the process eliminates duplicate risks from the Risk List and links risks where there may be an advantage in addressing these risks together for purposes of risk planning. Finally, based upon the primary outputs of the risk analysis, the risks are prioritized with the prioritization documented in the Risk List.

2.4 Risk Planning (Handling, Treatment, or Decisionmaking)

2.4.1 Risk Planning Concept.

Once the risks have been identified and analyzed, the next step is to plan the action that should be taken on each risk. In this case, the PM should at least ask the following questions:

"What can we do to prevent it from going wrong, or at least reduce the probability or severity of the consequences?"

"Who should be assigned to take these preventive actions?"

As described in NPR 7120.5, risk planning consists of assigning responsibility to determine the approach to respond to the identified risks and, if a decision is made to mitigate the risk, the subsequent development and implementation of the action to mitigate the risk. As each identified risk is assigned to a member of the program/project team or matrixed professional from another organization, it is that person's responsibility to determine the approach to respond to each assigned risk. The approaches for responding to risk are as follows:

a. Mitigate. Risk mitigation may be achieved by applying methods aimed at eliminating the risk or reducing the likelihood and/or consequence of a risk. This may be accomplished through engineering, schedule, or budgetary changes to designs, processes, or procedures; or alternate paths and approaches.

b. Accept. The PM shall establish the criteria for accepting risks, document the rationale for accepting individual risks and include the signed formal acceptance within the risk acceptance records. (Requirement 26025). One criteria for accepting risk is to have a documented, tested, and signed contingency or recovery plan in place to respond to the consequences of an accepted risk should that risk manifest itself as an undesired event.

c. Research. This includes the collection of additional information, evaluation, and reporting of results on which to base future decisions or, sometimes, to reduce the uncertainty surrounding risk estimates.

d. Monitor. This includes deciding not to take immediate action, but to track, survey, or watch the trends and behavior of risk indicators over time. If the mitigate approach is selected, the person assigned to the risk is responsible for determining the level of the scope of the mitigation, establishing the goal(s) of the mitigation effort and determining the resources required to implement the mitigation. (The scope of the mitigation includes the development of either an action item or a detailed task plan, both of which are referred to as risk mitigation plans). In addition, the person assigned to the risk is responsible for coordinating mitigation activities with the person who initially identified the risk, appropriate functional offices, and other persons assigned responsibilities for risks to ensure that the mitigation activities address all concerns and do not increase or introduce additional risk in another area.

2.4.2 Risk Planning Inputs.

The basic inputs to Risk Planning are the outputs from Risk Identification and Risk Analysis elements of the overall risk management process. The primary new input is the resources available within the program to be applied to mitigation action items or task plans. Development and implementation of the risk mitigation plans or, in the case of a risk acceptance decision, contingency or recovery plans, may be constrained by the resources available. Program/projects will want to carefully determine which mitigations provide the most improvement in risk. Analytical tools, such as cost-benefit analysis and PRA, can assist in helping to determine how to allocate limited resources among the mitigation actions that can provide the optimal improvement to the program/project's risk posture.

2.4.3 Risk Planning Outputs.

The outputs of risk planning are as follows:

a. Updates to the Risk List (see paragraph 2.7.6) to identify the assignment of a person to respond to the risk, and the identification of what action is to be taken with respect to the risk.

b. Individual risk mitigation plans (see paragraph 2.7.7), linked to the risk list, for each risk involving a decision to mitigate.

c. In the case of a decision to accept the risk, the acceptance rationale as included in the risk acceptance records (see paragraph 2.7.8).

2.5 Risk Tracking (Monitoring or Verification)

2.5.1 Risk Tracking Concept.

Risk tracking is used to measure the progress of the risk management program. In this area the PM should ask at least the following questions:

- "Are risk mitigation actions effectively mitigating risk and are the actions within budget and schedule constraints?"

- "Is the overall risk for the program/project increasing or decreasing?"

- "If the overall risk for the program/project is decreasing is it decreasing to the maximum practicable extent?

Risk tracking involves collecting, updating, compiling, organizing and analyzing risk data and reporting risk trends to determine whether particular risks are decreasing, staying the same, or increasing over time. Tracking focuses primarily on risks identified for mitigation, research, and monitoring, although all risks, including accepted risks, should also be tracked to ensure that conditions or assumptions have not changed to the point that reevaluation is necessary. For research actions, tracking serves to assure that the research efforts are progressing satisfactorily and that the identified timeframe still permits further research. Risk tracking should provide the insight on which to draw conclusions about the effectiveness of mitigation actions, or the need to take action on monitored risks that are increasing toward or beyond a trigger level. "Trigger" levels are the warning or control limits often used in statistical process control. Trigger levels (see Appendix A, Glossary) may be predetermined for particular risks (if the risks are being monitored) to signal the need for action. Trigger levels also identify those effects on the overall program/project, not only relative to the critical path but also to the resources and performance results; critical decisionmaking points; variations on systems capabilities; and other elements. Tracking results should be made readily available to the program/project team members. The frequency for checking tracking results and trigger levels should be such that the program/project team will have adequate time to react to adverse trends.

2.5.2 Risk Tracking Inputs.

Tracking of a particular risk requires knowledge of its data elements (including any metric(s)) from the Risk List, the applicable mitigation plan or tracking requirements (for watched risks), resources available for mitigation, and possibly other relevant program/project data (such as cost and schedule variances, critical path changes, and program/project performance indicators).

2.5.3 Risk Tracking Outputs.

The outputs of risk tracking are primarily risk status reports on the current program/project risk posture (see Appendix A, Glossary).

2.6 Risk Control (Feedback)

2.6.1 Risk Control Concept.

Risk control is the feedback process of reevaluating, based on recent tracking information, what actions to take concerning a particular risk, and implementing those decisions. The PM should be asking at least the questions:

"What risks still need to be researched?"

"What risk mitigations need to be revised?"

"Have risks reached a point (trigger level) where a contingency plan needs to be invoked?"

"What risks can be accepted and formally closed?"

Actions may include changing the current action plan, closing the risk (accepting the residual risk), invoking a contingency plan when the original plan is found to be ineffective, or continuing with the original plan and continuing to track the risk. Each of the risks identified, analyzed, planned, and tracked should be periodically reviewed (preferably monthly) to ensure that decisions made are effective and that associated actions remain applicable. Since NPR 7120.5 requires that **all** risks be dispositioned before delivery to operations, or the equivalent for a technology program, the program/project shall review and ensure that **all** risks are dispositioned before this milestone (Requirement 20631).

2.6.2 Risk Control Inputs.

All of the information developed as a part of the risk management process to this point, including the risk list and the risk mitigation plans, form the inputs to risk control.

2.6.3 Risk Control Outputs.

The outputs from risk control are decisions made by the PM, or appropriate decisionmaker, with respect to risk. The decisions reflect the program/project's authorization to apply one of the approaches for responding to risk identified within the risk planning element of the risk management process. Decisions, or revalidation of those decisions, to mitigate, research, or monitor risk would be documented in accordance with program practices and would be reflected within the Risk List. The decision to close an identified risk shall be formally documented with signatures of the PM, the person having assigned responsibility for the risk, and the person that identified the risk (Requirement 26033). In addition, the GPMC must concur with the acceptance of all primary risks (Requirement 30909).

2.7 Documenting and Communicating Risk

2.7.1 General.

Effective RM requires open, clear, and ongoing communication within the program/project team. The RM documentation process ensures that RM policies are established, understood, implemented, and maintained, and that a formal audit trail is developed to establish the origin of, and rationale for, all risk-related decisions. RM documentation shall be readily accessible to the entire team; e.g., in an automated form, and under configuration control. , (Requirement 26034). The RM process draws on existing project documentation to the maximum extent possible. RM documentation and records are maintained in accordance with the requirements of NPD 1440.6, "NASA Records Management," and NPR 1441.1, "Records Retention Schedules," and as documented in the Risk Management Plan. In addition to the requirements of NPD 1440.6 and NPR 1441.1, documentation of the inputs, analyses, and outputs of each element of the RM process may also be considered by the Center to be quality records as defined by ANSI/ASQC Q9001-1994.

2.7.2 Program/Project Plan.

The Program/Project Plan, as required by NPR 7120.5, includes a summary of the basic risk management planning for the program/project. The implementation of the basic strategy/philosophy for program/project risk management described in the Program/Project Plan is then further detailed within the Risk Management Plan. The Program/Project Plan is also the location where the acceptable risk (see Appendix A, Glossary) level for the program/project is defined and documented and a summary of the primary risks for the program/project is documented.

2.7.3 Acquisition Plan.

The Acquisition Plan, developed in conjunction with the Acquisition Strategy Meeting, is required by the NASA FAR Supplement (NFS) 1807.105. The requirements for the Acquisition Plan include many risk management items. Specifically, the Acquisition Plan is required to do three things related to risk management. First, it discusses the Program's/Project's risks (including a quantification (magnitude of risk). Second, it discusses how to structure the acquisition approach to manage risks, and third, it identifies decisions made to accept, mitigate, track and/or research acquisition risks. The Risk List (paragraph 2.7.6), Risk Acceptance Records (paragraph 2.7.8), and Risk Mitigation Plans (paragraph 2.7.7) provide the core data to develop the risk management portions of the Acquisition Plan and support completion of the Acquisition Strategy Meeting.

2.7.4 Risk Management Plan.

2.7.4.1 Risk Management Plan General.

As specified in NPR 7120.5, "NASA Program and Project Management Processes and Requirements," every program/project shall have an RM Plan (Requirement 26037). This stand-alone plan, approved by the PM during the Formulation Subprocess, should be an integral element of the program/project documentation. The RM Plan shall be placed under formal configuration control (Requirement 30910). The RM Plan should be reviewed and updated as necessary when a change in program phase occurs, or when significant changes in success criteria, program architecture, or design occur. The RM Plan shall be available for review by the GPMC (Requirement 30911). Note: In developing the Risk Management Plan, keep in mind that other requirements and guidance such as those documented in the NFS, NPR 2810.1, "Security of Information Technology," and NPR 8715.3, "NASA Safety Manual," will need to be considered and addressed accordingly.

2.7.4.2 Risk Management Plan Content.

2.7.4.2.1 The RM Plan shall be program/project specific, configuration controlled, and include the following (incorporating technical information by reference) (Requirement 26038).:

a. Introduction. Explain the purpose, scope, assumptions, success criteria, constraints, processes, and key ground rules pertaining to the program/project RM process.

b. Overview of Risk Management Process. Provide an overview of the RM process and information flow; describe how the RM process integrates and relates to other program/project management activities. Include general risk mitigation strategies to be employed throughout program/project implementation.

c. Organization. Provide an explanation of the organization, roles, and responsibilities of the program/project with respect to risk management. Provide a clear indication of where and how customers and suppliers interact with the organization, including specific responsibilities if appropriate. Consider the use of a Responsibility Assignment Matrix to help document the responsibilities. Provide an explanation of how team members will be trained in the application of RM methodology.

d. Process Details. Provide the RM process details and related procedures, methods, tools, and metrics. Identify the process and considerations to be used in determining the level of indenture to which the risk analyses are to be conducted. Include in this section, or in an appendix, the specific methodologies to be used for risk identification, analysis, planning, tracking, and controlling. Include the process to be used for prioritization of risk, identification of risk acceptance criteria, application of resources to risks, and continual assessment of the program/project risk profile. Describe how risk information will be communicated both internally to the program/project staff and throughout the management chain. Document links to other risk-related requirements, processes, and products, such as processes and products defined within related IT Security Plans as required by NPR 2810.1 and Acquisition Plans required by the NASA FAR Supplement.

e. Resources and Schedule of Risk Management Milestones. Show schedule, milestones, and allocation of resources for RM activities, including resource reserves (contingency) that might be available for risk mitigation.

f. Documentation of Risk Information. Specify the format and data elements that will comprise the program/project Risk List (see paragraph 2.7.6 for a suggested format). Document where and how the list will be maintained, how configuration control will be applied, how the list will be used, and how often it will be updated/reviewed. Tell how team members will be able to access the current list at any time. When applicable, address intra- as well as inter-programmatic considerations; e.g., spacecraft-to-spacecraft and spacecraft-to-environmental systems dependencies, resources outside the program/project's control such as wind tunnel access, test facilities, launch facilities, support aircraft, IT resources that are vital to the success of the program, which might affect risk. (Recommend that the format be set, with a minimal number of elements, to allow database compilation). Specify the format, content, and schedule of all other RM documentation used within the program/project, such as Risk Mitigation Plans and Risk Acceptance Records.

g. Methodology Associated with Program/Project Descope. Discuss the program/project descope (see Appendix A, Glossary) methodology that might be applied when risk mitigation cannot be accomplished due to limited resources (cost, schedule, workforce). Note: Limited resources are not an excuse for not meeting legislated or otherwise mandated requirements. This discussion should include identification of organizations that would be impacted by the identified descoping (for example, if the descoping involved changes to contracts, the appropriate procurement organizations would need to be involved). Describe the point in the descoping process at which the program/project would no longer meet sufficient mission objectives or success criteria to be considered viable.

2.7.4.2.2 The CRM website, http://crm.nasa.gov/ and the Process Based Mission Assurance Knowledge Management System, http://pbma.hq.nasa.gov/ contain sample RM plans, a template for preparing them, and additional templates for tailoring RM to a specific project, whether large or small.

2.7.5 Statement of Risk.

The Statement of Risk is a clear, concise, and complete statement of the risk. In general, risk statements are written in a condition - consequence format (that is "given the there is a possibility that will occur"). It can be supported by additional information if required to place the risk in context or explain the assumptions associated with the risk. If supporting information is required the Statement of Risk should be clearly linked to that information and where it is maintained.

2.7.6 Risk List.

2.7.6.1 Every program/project shall have a Risk List. (Requirement 26065). The Risk List is the listing of all identified risks in priority order from highest to lowest risk, together with the information that is needed to manage each risk and document its evolution over the course of the project. Risk prioritization is performed by the project team and consolidated and approved by the PM. Figure 3 provides suggested data elements and format for the Risk List.

Priority	Risk Statement	Risk Tracking Identifier	Risk Originator	Consequence	Likelihood	Timeframe	RAC	Classification	Primary Risk	Responsible Person
1										
2										
3										
4										

Figure 3. Risk List

KEY:

Priority - Enter the priority for the identified risk.

Risk Statement - Enter a clear, concise statement of the risk. If additional information is required to place the risk in context or explain the assumptions associated with the risk, identify where that information is maintained.

Risk Tracking Identifier - Provide a unique identifier for the risk for tracking purposes.

Risk Originator - Identify the person who identified the risk and can provide background information concerning the risk.

Consequence - Identify the consequence of the risk (including, but not limited to cost, performance, schedule impact, and personnel illness/injury).

Likelihood - Identify the likelihood of the risk occurring.

Timeframe - Identify the timeframe when action on the risk needs to be completed.

RAC - Enter the appropriate RAC for the identified risk.

Classification - Identify any subdivisions or groupings of risks.

Primary Risk - Indicate if the risk is a primary risk (yes/no).

Responsible Person - Identify the person assigned to provide the risk response.

Risk Response - Identify what response has been designated for the risk (Mitigate, Accept, Research, Monitor). If a risk has been accepted, identify where the risk acceptance is documented. If a risk is mitigated, identify the appropriate risk mitigation plan.

Metrics - Identify any metrics related to the risk that are being used for tracking/trending.

2.7.6.2 The Risk List must be updated as changes (including changes in assumptions) occur (Requirement 26063). Extracts from the list shall be presented at project meetings, reviews, and milestones as required by the RM Plan (Requirement 30912). Programs/projects may also find it beneficial to use the classification of risks to create subsets of the Risk List in addition to the complete Risk List so that working or functional groups may focus on specific areas of risk (for example, tracking all of the environmental risks or the security risks or technical risks together). The Risk List must be widely accessible to all members of the program/project team (Requirement 30913).

2.7.7 Risk Mitigation Plans.

These plans describe actions to mitigate identified risks, as well as risk measures, indicators, and trigger levels used in the tracking of the risks and the effectiveness of their mitigation actions. These plans also include the cost and schedule information required to implement the plan. The program/project determines the format for the plans (which could range from simple action items for relatively simple mitigations to formal task plans for more complex mitigations) consistent with other program/project planning documentation.

2.7.8 Risk Acceptance Records.

These records document program/project acceptance of risk (and, if a primary risk, GPMC concurrence). The program/project determines the format of these records consistent with other program/project documentation (for example, program/project configuration management processes and documentation could be used to document acceptance of risk). The risk acceptance records include the risk acceptance rationale, as well as the appropriate signatures for approval, including revalidations as required.

2.7.9 Risk Trends.

These consist of displays (graphical, tabular, or textual) showing changes to risk indicators over time; i.e., decreasing, staying the same, or increasing. Trends should be updated frequently, on a schedule documented in the RM Plan, so that the program/project team will have adequate time to react to adverse trends. Risk trend documentation should also be consistent with other program/project metrics information.

2.7.10 Risk Profile.

Beginning early in a project, the PM should make a qualitative or quantitative projection of overall expected risk trend (technical risks, as well as programmatic risks) over the life of the program/project (showing major milestones). A risk profile such as the example shown in Figure 4 should be constructed. Initially, the projected risk profile (that part that lies in the future) should be annotated to explain significant, but expected, changes in risk. Over the life of a program/project, the risk profile should be updated regularly, as documented in the RM Plan, to reflect actual changes in risk. Explanations for these changes should be annotated on the profile for briefing at major milestone meetings.

MARS PATHFINDER RISK PROFILE
SCHEDULE/COST AND MISSION RISK

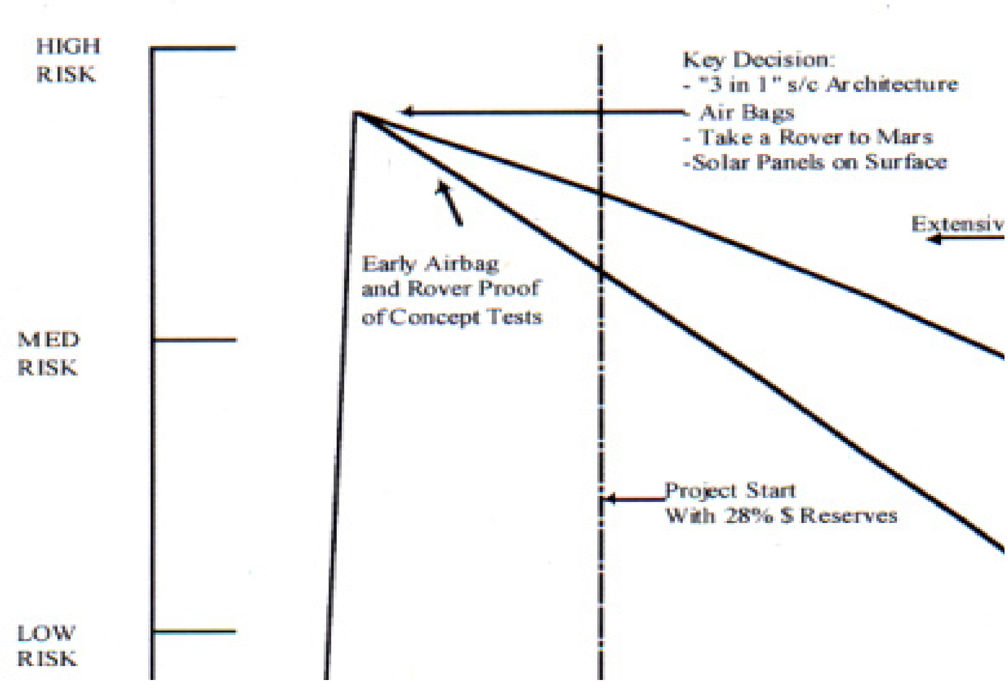

Figure 1. Continuous Risk Management (CRM)
Print

Figure 4. Risk Profile Example (Mars Pathfinder, constructed post-mission)

Note: The terms Technical and Programmatic Risk used in this NPR are roughly equivalent to the terms Mission Risk and Cost/Schedule Risk, respectively as they are used in this figure.

2.7.11 Risk Communication.

2.7.11.1 Early in a program/project, the PM should develop a risk communication strategy. It should address how risk will be openly and clearly communicated within the program/project team, with management, stakeholders, appropriate functional offices, other government entities, and the public, throughout the life cycle of the program/project.

2.7.11.2 Consideration should be given to establishing a program/project RM database to provide an easily accessible way to store program/project risk information and thereby aid every step of the RM process. This would also provide a risk record archive, making tracking and analyzing risk, past methods, and results available for all to view.

| TOC | ChangeHistory | Preface | Chp1 | Chp2 | AppdxA | AppdxB | AppdxC | AppdxD | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS